ABSTRACT

Improvements Relating To Quantum Cryptography

A method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel is described. The method comprises: generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space, transmitting the plurality of random quantum states of the quantum entity via the quantum channel to a recipient, measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space, transmitting to the recipient composition information describing a subset of the plurality of random quantum states, analysing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states, establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar, deriving a first binary string and a second binary string, correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset, and carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings.